GUIDANCE NOTES (AMENDMENTS) ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

Section 3

ASSESSING RISK AND APPLYING A RISK BASED APPROACH

A. INTRODUCTION

1. The purpose of this section is to provide guidance to FSPs on applying a risk-based approach to their anti-money laundering/countering terrorist financing (AML/CFT) framework.

B. THE RISK-BASED APPROACH[1]

1. The AMLRs require FSPs to apply a risk-based approach (RBA) to their AML/CFT framework. The adoption of an RBA is an effective way to prevent or mitigate money laundering and terrorist financing (ML/TF) as it will enable FSPs to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. As such, FSPs should develop an appropriate RBA for their particular organisation, structure and business activities. Where appropriate and feasible, the RBA should be articulated on a group-wide basis.

2. As is the case for an FSPs' overall risk management, FSPs' senior management should understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks.

3. FSPs shall, before determining what the level of overall risk is and the appropriate level and type of mitigation to be applied, consider all the relevant risk factors. This would include the risks that are identified at the national level through the National Risk Assessment (NRA) or similar assessment, or risk assessment conducted by the relevant Supervisory Authority, whichever is most recently issued.

4. FSPs should at the outset of the relationship understand their business risks and know who their applicants for business ("applicants")/customers are, what they do, in which jurisdictions they operate, and their expected level of activity with the FSP.

[1]FATF R.1 and IO.1

5. FSPs in conducting their risk assessments should take into account all relevant information from various sources including, but not limited to:
   (1) the Cayman Islands' NRA of ML/TF;
   (2) the NRA of other jurisdictions in which the FSPs have subsidiaries or customers;
   (3) reports from law enforcement agencies and the Financial Reporting Authority;
   (4) guidance, circulars and other communication from the Monetary Authority or other relevant authorities;
   (5) information from industry associations;
   (6) information from international standard setting bodies such as FATF; and
   (7) other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by an FSP on a risk sensitive basis.

6. Following their risk assessment, FSPs should categorise their business relationships and occasional transactions according to the perceived level of ML/TF risk. Each FSP should decide on the appropriate way to categorise risk.

7. As a part of the RBA, FSPs shall:
   (1) identify ML/TF risks relevant to them;
   (2) assess ML/TF risks in relation to:
      (a) their applicants/customers (including beneficial owners);
      (b) Country or geographic area in which persons under (a) above reside or operate and where the FSP operates;
      (c) products, services and transactions that the FSP offers; and
      (d) their delivery channels[2].

   (3) design and implement policies, controls and procedures that are approved by senior management to manage and mitigate the ML/TF risks that they identified under (1), commensurate with assessments under (2) above;
   (4) evaluate mitigating controls and adjust as necessary;
   (5) monitor the implementation of systems in (3) above and improve systems where necessary;
   (6) keep their risk assessments current through ongoing reviews and, when necessary, updates;
   (7) document the RBA including implementation and monitoring procedures and updates to the RBA; and
   (8) have appropriate mechanisms to provide risk assessment information to competent authorities.

8. Under the RBA, where there are higher risks, FSPs are required to implement enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high-risk situations or situations which are outside the FSP's risk tolerance, the FSP may decide not to take on the applicant/customer, or to exit from the relationship.

C. IDENTIFICATION AND ASSESSMENT OF RISKS

1. When identifying and assessing risk, FSPs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. ML/TF risks should be measured considering all available relevant information.

[2] Delivery channel in this context is the way/means whereby an FSP carries its business relationship with a customer, e.g. directly or through other means such as email, internet, intermediary, or any correspondent institution.

2. FSPs should identify and assess the inherent and residual risks they face with regard to their products, services, delivery channels, customer types, geographic locations in which they or their customers operate and any other relevant risk category.

3. ML/TF risks may be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk. For example, one of the risk factors that may be relevant when considering the risk associated with its customers whether a customer issues bearer shares[3] or has nominee shareholders.

4. FSPs should consider all relevant risk factors for each risk category before determining the overall risk classification (e.g. high, medium or low) and the appropriate level of mitigation to be applied.

5. FSPs should make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, FSPs should take into consideration the relevance of different risk factors in the context of a particular customer relationship or occasional transaction. Examples of the application of various factors to the different categories that may result in high and low risk classifications are provided below. When weighting risk, FSPs should ensure that:
   (1) weighting is not unduly influenced by any one factor;
   (2) economic considerations do not influence the risk rating;
   (3) situations do not arise where it is not possible for any business relationship to be classified as high risk;
   (4) situations which are identified by relevant legislation as always presenting high ML/TF risks, are not overruled by the FSPs weighting; and
   (5) FSPs are able to override any automatically generated risk score, where necessary.

6. FSPs may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

7. FSPs should document their risk assessment in order to be able to demonstrate their allocation of compliance resources, keep these assessments up-to-date and have appropriate mechanisms to provide risk assessment information to the relevant Supervisory Authority (and competent authorities and self-regulatory bodies ("SRBs"), if required). The nature and extent of any assessment of ML/TF risks should be appropriate to the nature, size and complexity of the business.

D. RISK CLASSIFICATION FACTORS

1. Risk classification factors may be categorised by types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

Customer Risk Factors

2. When identifying the risk associated with their customers, including their customers' beneficial owners, FSPs should consider the risk related to the customer's and the customer's beneficial owner's:

[3] Note that bearer shares are not permitted under the laws of the Cayman Islands.

(1) business or activity;
(2) reputation insofar as it informs about the customer's or beneficial owner's financial crime risk; and
(3) nature and behaviour.

3. These factors considered individually may not be an indication of higher risk in all cases, however a combination of them may warrant greater scrutiny.

High-risk Classification Factors (Customer)

4. FSPs should consider the following high-risk factors when assessing customer risk with regard to:
   (1) customer's business or activity when:
      (a) the customer is connected to sectors that are commonly associated with higher ML/TF/PF, such as cash-intensive businesses;
      (b) the customer is a politically exposed person (PEP);
      (c) the customer is a public body or state-owned entity from a jurisdiction with high levels of corruption;
      (d) the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the FSP and the applicant/customer);
      (e) legal persons or arrangements that are personal asset-holding vehicles;
      (f) companies that have nominee shareholders or shares in bearer form[4]; and
      (g) the customer has a background which is inconsistent with what the FSP's records.

   (2) reputation insofar as it informs about the customer's or beneficial owner's financial crime risk when:
      (a) the customer holds a prominent position or enjoys a high public profile that might enable them to abuse this position for private gain;
      (b) there are adverse media reports or other relevant sources of information about the customer (e.g. there any allegations of criminality or terrorism against the customer which are reliable and credible);
      (c) the customer or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing;
      (d) the customer has been the subject of a suspicious activity report in the past; and
      (e) the FSP has any in-house information about the customer integrity, obtained, during the course of the business relationship.

   (3) nature and behaviour, where:

      (a) the customer is unable to provide robust evidence of their identity;
      (b) the FSP has any doubts about the veracity or accuracy of the customer's identity;
      (c) the ownership structure of the applicant/customer appears unusual or excessively complex given the nature of the applicant/customer's business.
      (d) there are indications that the customer might seek to avoid the establishment of a business relationship (e.g. the customer seeks to carry out a number of separate wire transfers, or other services and does not open an account, where

[4] FSPs are reminded that Cayman Islands Companies are not allowed to issue shares in bearer form. Please refer to the Companies Law for further guidance. As a best practice, FSPs should restrict themselves from conducting business with persons whose shares are in bearer form.

the establishment of a business relationship might make more economic sense);

(e) the customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale;
(f) the customer requests unnecessary or unreasonable levels of secrecy (e.g. the customer is reluctant to share CDD information, or appears to want to disguise the true nature of their business);
(g) the customer's source of wealth or source of funds cannot be easily explained;
(h) the customer does not use the products and services it has taken out as expected when the business relationship was first established;
(i) the customer is a non-profit organisation whose activities could be abused for terrorist financing purposes;
(j) the risk posed by the combination and complexity of products, services and delivery channels that the applicant/customer uses;
(k) the risk posed by the geographical location of the applicant/customer (e.g. countries in which the applicant (and its beneficial owner) resides or from which it operates); and
(l) the risk posed by the customer's characteristics, nature and purpose of the relationship or nature of transaction.

Low-Risk Classification Factors (Customer)

5. When assessing customer risk, FSPs may consider the low-risk classifications for applicants/customers that satisfy the requirements under regulation 22 (d) of the AMLRs.

Country/Geographic Risk Factors

6. Country/geographic risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. FSPs should consider jurisdictions they are exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and listed by FATF.

High-risk Classification Factors (Country/geographic area)

7. When identifying higher risks relating to country/geographic areas, FSPs should consider:

(1) whether the country has been identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems;
(2) whether the country is subject to sanctions, embargos or similar measures issued (e.g., sanctions imposed by the United Nations);
(3) whether the country or geographic area has been identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their jurisdiction;
(4) the nature and purpose of the customer's business relationship within the jurisdiction;
(5) the level of ML/TF risk within the jurisdiction;
(6) the level of predicate offences relevant to money laundering within the jurisdiction; and
(7) the level of legal transparency and tax compliance within the jurisdiction.

Low-risk Classification Factors (Country/geographic area)

8. In identifying lower risks relating to country/geographic areas, FSPs may consider:
   (1) countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems; and
   (2) countries identified by credible sources as having a low level of corruption or other criminal activity.

Product, Services and Delivery/Distribution Channels Risk Factors

9. The overall risk assessment of an FSP should include determining the potential risks presented by products, services and delivery channels it offers. When assessing the risk associated with their products, services or transactions, FSPs should consider the level of transparency, or opaqueness, the product, service or transaction affords; the complexity of the product, service or transaction; and the value or size of the product, service or transaction.

10. When identifying the risk associated with delivery channels, FSPs should consider the risk factors related to the extent that the business relationship is conducted on a non-face to face basis; and any introducers or intermediaries it utilises and the nature of those relationships.

High-risk Classification Factors (Products, services and delivery channels)

11. When assigning high risk ratings relating to products, services and delivery channels, FSPs should consider:
   (1) the level of transparency, or otherwise of the product, service or transaction (e.g. the extent to which the products or services facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures that could be used for illicit purposes);
   (2) non-face-to-face business relationships or transactions (e.g. if the customer is not physically present for identification purposes, whether the FSP uses reliable forms of non-face-to-face CDD);
   (3) payments received from unknown or unassociated third parties;
   (4) the value or size of the product, service or transaction (e.g. the extent that the products or services may be cash intensive, or the extent that the products or services facilitate or encourage high value transactions);
   (5) the complexity of the product, service or transaction, including the use of new technologies or payment methods;
   (6) whether, in the case of insurance products/services, there is a surrender of single premium life product or other investment-linked insurance products with a surrender value;
   (7) enhanced scrutiny of other activities, products or services such as private banking, trade finance payable through accounts, trust and asset management services, prepaid cards, remittance, lending activities (loans secured by cash collateral) and special use or concentration accounts

Low-risk Classification Factors (Products, services and delivery channels)

12. In assigning lower risk classifications relating to products, services and delivery channels, FSPs may consider:

(1) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion[5]purposes;
(2) products and services that do not encourage early surrender options (e.g. in the case of insurance policies for pension schemes);
(3) products that cannot be used as collateral; and
(4) products that with strict rules that do not permit the assignment of a member's interest (e.g. a pension, superannuation or similar scheme, where contributions are made by way of deduction from wages).

13. The examples of risk factors/indicators outlined are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

E. RISK MANAGEMENT AND MITIGATION

Risk Tolerance

1. Risk tolerance is the amount of risk that the FSP is willing and able to accept. An FSP's risk tolerance is an important component for achieving effective risk management and impacts its decisions about risk mitigation measures and controls. For example, if an FSP determines that the risks associated with a particular type of customer exceed its risk tolerance, it may decide not to accept or maintain that particular type of customer(s). Conversely, if the risks associated with a particular type of customer are within the bounds of an FSP's risk tolerance, the FSP must ensure that the risk mitigation measures it applies are commensurate with the risks associated with that type of customer(s).

2. FSPs should establish their risk tolerance. Such establishment should be done by senior management and the Board. In establishing the risk tolerance, the FSP shall identify the risks that it is willing to accept and the risks that it is not willing to accept. It should consider whether it has sufficient capacity and expertise to effectively manage the risks that it decides to accept.

3. When establishing the risk tolerance, an FSP should consider consequences such as legal, regulatory, financial and reputational consequences of an AML/CFT/PF compliance failure.

4. If an FSP decides to establish a high-risk tolerance and accept high risks then the FSP should have mitigation measures and controls in place commensurate with those high risks.

Risk Management and Mitigation

[5] In general terms, financial inclusion involves providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the formal financial sector. Financial inclusion also involves making a broader range of financial products and services available to individuals who currently only have access to basic financial products. Financial inclusion can also be defined as ensuring access to appropriate financial products and services at an affordable cost in a fair and transparent manner. For AML/CFT/PF purposes, it is essential that these financial products and services are provided through financial institutions subject to adequate regulation in line with the FATF Recommendations. Examples of such products/services can include basic/low amount savings accounts, school children savings accounts. For additional information see the FATF's Guidance "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion."

5. FSPs should have appropriate policies, procedures and controls that enable them to manage and mitigate effectively the risks that they have identified, including the risks identified by the country. They should monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements.[6]

6. The policies and procedures designed to mitigate assessed ML/TF/PF risks should be appropriate and proportionate to these risks and should be designed to provide an effective level of mitigation.

7. The nature and extent of AML/CFT/PF controls will depend on a number of aspects, which include:

   (1) the nature, scale and complexity of the FSP's business;
   (2) diversity, including geographical diversity of the FSP's operations;
   (3) FSP's customer, product and activity profile;
   (4) volume and size of transactions;
   (5) extent of reliance or dealing through third parties or intermediaries.

8. Some of the risk mitigation measures that FSPs may consider include:

   (1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, products or a combination of both;
   (2) setting transaction limits for higher-risk customers or products;
   (3) requiring senior management approval for higher-risk transactions, including those involving PEPs;
   (4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;
   (5) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

Evaluating Residual Risk and Comparing with the Risk Tolerance

9. Subsequent to establishing the risk mitigation measures, FSPs should evaluate their residual risk. Residual risk is the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the FSP's overall risk tolerance. Where the FSP finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high risks, the FSP should enhance the risk mitigation measures that are in place.

F. MONITORING AML/CFT SYSTEMS AND CONTROLS

1. FSPs will need to have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. FSPs shall update their systems as appropriate to suit the change in risks.

[6] FATF R.1 and IN- 9

2. Additionally, FSPs shall assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. For that purpose, the FSP will need to consider monitoring certain aspects which include:

   (1) the ability to identify changes in a customer profile or transaction activity/behaviour, which come to light in the normal course of business;
   (2) the potential for abuse of products and services by reviewing ways in which they may be used to facilitate ML/TF/PF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
   (3) the adequacy of staff training and awareness;
   (4) the adequacy of internal coordination mechanisms, that is, between AML/CFT compliance and other functions/areas;
   (5) the compliance arrangements (such as internal audit or external review);
   (6) the performance of third parties who were relied on for CDD purposes;
   (7) changes in relevant laws or regulatory requirements; and
   (8) changes in the risk profile of countries to which the FSPs or its customers are exposed to.

G. NEW PRODUCTS AND TECHNOLOGIES

1. FSPs should have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:

   (1) digital information storage including cloud computing;
   (2) digital or electronic documentation storage;
   (3) electronic verification of documentation;
   (4) data and transaction screening systems; or
   (5) the use of virtual or digital currencies.

2. Electronic money systems for example, may be attractive to money launderers or those financing terrorism if the systems offer liberal balance and transaction limits, but provide for limited monitoring or review of transactions. FSPs may also face increased difficulty in applying traditional AML/CFT/PF measures because of the remote access by customers of the systems.

3. Systems utilizing new technologies that are involved with the collection, monitoring or maintenance of customer information for example, may not be as reliable or work as expected or may not be fully understood by staff. Such systems could therefore be vulnerable and result in FSPs not complying with the AMLRs.

4. FSPs should also:
   (1) undertake a risk assessment prior to the launch or use of such products, practices and technologies; and
   (2) take appropriate measures to manage and mitigate the risks.[7]

5. FSPs should have policies and procedures in place or such measures as may be needed to prevent the misuse of technological development in ML/TF/PF schemes, particularly those technologies that favour anonymity. Banking and investment business on the Internet, for example, add a new dimension to FSPs' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF/PF, and fraud.

[7] FATF- R. 15 and Methodology 15.1 and 15.2

6. It is recognized that on-line transactions and services are convenient. However, it is not appropriate that FSP should offer on-line live account opening allowing full immediate operation of that account in a way which would dispense with or bypass normal identification procedures.

7. However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied in accordance with these Guidance Notes.

8. The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities. The fast pace of technological and product development has significant regulatory and legal implications, and FSPs must ensure that appropriate staff members keep abreast of relevant technological developments and identified methodologies in ML/TF/PF schemes. This may involve reviewing papers from international bodies such as the FATF on AML/CFT/PF typologies, warnings and information issued by regulators and law enforcement, as well as information issued by industry bodies or trade associations.

9. To maintain adequate systems, FSPs should ensure that its systems and procedures can be and are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by the FSPs. Risks identified must be fed into the FSPs' business risk assessment.

H. EMERGING RISKS

1. FSPs should ensure that they have systems and controls in place which identify and assess emerging ML/TF/PF risks and incorporate them into their assessments in a timely manner. Where a FSP is aware that a new risk has emerged, or an existing risk has increased or otherwise changed, the changes should be reflected in the risk assessment as soon as possible.

I. DOCUMENTATION

1. FSPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the FSP to demonstrate to the relevant Supervisory Authority and/or to a court:

   (1) risk assessment systems including how the FSP assesses ML/TF/PF risks;
   (2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
   (3) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
   (4) the arrangements for reporting to senior management on the results of ML/TF/PF risk assessments and the implementation of its ML/TF/PF risk management systems and control processes.

J. REVIEW OF THE RISK ASSESSMENT

1. The AML/CFT risk assessment should be subjected to regular reviews to ensure that it adequately reflects the ML/TF risks pertaining to the FSP. FSPs should also assess information obtained as part of their ongoing monitoring business relationships and

consider whether this affects the risk assessment. It is the expectation of the Monetary Authority that these reviews are approved by the Board of the FSP.